International Working Group
on Data Protection
in Telecommunications

675.43.18

13 September 2011

Working Paper

Privacy by Design and Smart Metering: Minimize Personal Information to Maintain Privacy

50th meeting, 12-13 September 2011, Berlin (Germany)

Background

With the ongoing growth of the Smart Grid, the role of the utility is changing. Historically, energy providers focused on maintaining consistent supply at the lowest possible cost; interactions with customers largely involved billing and minimizing credit risk. However, with the current redesign of electrical systems, these interactions are being radically redesigned, as smart meters allow utilities to gain information about the usage patterns of their residential customers at a level of detail that was previously unavailable, and in near real-time. This change is allowing for the development of an array of new services and efficiencies for both the consumer and the utility.

To maintain consumer trust and confidence, the Smart Grid and smart metering will necessitate the emergence of a new relationship between utilities and individuals, centred on customer engagement. Privacy and data security will be the dual cornerstones of this relationship.

Smart Meters

When looking at the Smart Grid, the technology that will be most apparent to consumers will be the smart meter – the "essential first step" toward the implementation of a broader Smart Grid as a whole.[1] These meters, which incorporate two-way communications and enhanced individual usage information, will allow energy consumers to control and regulate their own consumption and utilities to enable demand response and load balancing functions. They will also play a key role in the development of improved power savings strategies to support the international fight against global warming, while allowing consumers to reduce consumption through information and feedback systems[2]. A 2009 Pike Research report suggests that 250 million smart meters could be installed worldwide by 2015.[3] These meters will play an integral role in utilities' overall Advanced Metering Infrastructures, which, while not further discussed here, will also require the incorporation of appropriate privacy protections at the system level.

[1] European Commission Staff Working Paper, Interpretative note on directive 2009/72/EC concerning common rules for the internal market in electricity and directive 2009/73/EC concerning common rules for the internal market in natural gas, p. 7, online: http://ec.europa.eu/energy/gas_electricity/interpretative_notes/doc/implementation_notes/2010_01_21_retail_markets.pdf

[2] Pacific Northwest National Laboratory: The Smart Grid: An Estimation of the Energy and CO_2 Benefits. http://energyenvironment.pnnl.gov/news/pdf/PNNL-19112_Revision_1_Final.pdf

[3] Pike Research (Nov. 2, 2009) "Smart Meter Installations to Reach 250 Million Worldwide by 2015", online: http://www.pikeresearch.com/newsroom/smart-meter-installations-to-reach-250-million-worldwide-by-2015

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

There is no standard, universal definition for the term 'smart meter'; in fact, the term has been applied to a variety of devices that incorporate different functionalities. There are, though, certain basic characteristics shared by most smart meters currently deployed. The most fundamental of these qualities is the digital metering of household energy consumption at a relatively fine level of granularity – minute-by-minute readings of energy used, for instance. Even a less fine level of granularity, such as hourly readings, allows for the collection of 'interval consumption' data which enables the possibility of Time-of-Use billing, by which different energy rates are applied based on the time at which energy was consumed. A digital readout displaying household energy consumption data (such as current or historic interval consumption) will generally be present, along with a means of communicating this information to another device (e.g. a smartphone or television). Smart meters may also be equipped with internal memory sufficient to enable the storage of all readings for at least a 6 month period.

Smart meters also tend to be equipped with bi-directional communication functionality. This allows utilities to remotely read the meters (at a significantly reduced cost as compared to meters being read onsite by a utility employee), and increasingly is enabling consumers to monitor their historic interval consumption via online web portals. Bi-directional communication also allows utilities to enable 'load balancing' functions, in which the utility can mediate energy consumption through communications with smart meters in participating households. In some jurisdictions, the consumer can install a special device on an appliance that automatically controls its energy consumption based on the network load. Some smart meters with bi-directional communication capabilities may also be equipped with remote enablement and disablement of supply functionality, enabling a utility to remotely connect or disconnect a consumer.

Although smart metering to date has been focused on electrical power consumption, it is anticipated that smart meters may also be used for water, gas and heat. Accordingly, some smart meters are being designed to support metering of multiple utilities in order to avoid unnecessary duplication of infrastructure.

Smart Meter Privacy Issues

Since its introduction, legislators, numerous privacy groups and regulatory agencies have focused on the need to protect consumer privacy in the Smart Grid[4]. The Smart Grid is expected to generate up to eight orders of magnitude more data than the current power network[5] which, in some cases, could reveal detailed information about a person. This increase in electrical consumption data is paired with remote reading and collection of the data, raising issues with regard to transparency and consumer control of data.[6]

Research suggests that as the Smart Grid matures, consumer lifestyles could be gleaned from the information generated – particularly as this information becomes more granular, and the power consumption signatures of appliances become recognizable. However, even if electricity use is not re-

[4] Examples include the German energy legislation (Energiewirtschaftsgesetz – EnWG, last amended on 28 July 2011, Bundesgesetzblatt I, S. 1690), the Information and Privacy Commissioner of Ontario, Canada's series of Smart Grid white papers, and The Article 29 Data Protection Working Party's "Opinion 12/2011 on Smart Metering (WP 183)." http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf

[5] "Accenture Launches Smart Grid Data Management Solution to Reduce Risks and Costs of Smart Grid Deployments," Mar. 18, 2010, online: http://newsroom.accenture.com/article_display.cfm?article_id=4971

[6] Resolution of the 80th Conference of the Data Protection Commissioners of the Federation and of the Länder (Nov. 3-4, 2010), "Data protection in connection with digital metering and control of energy consumption." http://www.datenschutz-berlin.de/attachments/823/Appendix_2.pdf

corded minute by minute, or at the appliance level, ongoing monitoring of electricity consumption may reveal the approximate number of occupants in a household, when they are present, as well as when they are awake or asleep. This may jeopardize the sanctity of the home, and such intimate details of daily life require a high level of protection. This information should not be accessible without the knowledge and consent of the occupant(s). The consumer must have the opportunity and ability to intervene and to determine who can access this data. In principle, any personal data disclosed must be minimized, in terms of both type and quantity of data disclosed and disclosure only to necessary parties.

The importance of maintaining consumer trust and confidence with respect to privacy and smart metering has been seen in numerous jurisdictions. Examples include:

- **California, USA**: Utility PG&E has faced blockades by residents looking to prevent the installation of smart meters in their neighbourhoods, citing privacy and health concerns.[7]
- **British Columbia, Canada**: Numerous complaints have prompted the province's Information and Privacy Commissioner to launch an investigation of BC Hydro's smart meter program, noting "the privacy and security of energy consumption data is a very real issue for citizens."[8]
- **Netherlands:** A 2006 bill proposing the mandatory rollout of smart meters was rejected, in part due to a report that found that the privacy concerns associated with the bill might have violated the Article 8, respect for one's private and family life, of the European Convention on Human Rights.[9]

In these cases and others, upfront initiatives to develop and communicate data privacy and protection measures for smart metering systems would have played a key role in avoiding deployment setbacks.[10]

Privacy by Design

Concurrent to the change in the consumer-utility relationship and the collection of increasing power usage information is the global adoption of the principles of *Privacy by Design* (*PbD*). From its origins in the mid-90s, *PbD* has become a worldwide standard, being recognized as "an essential component of fundamental privacy protection" through an International Resolution unanimously passed at the International Data Protection and Privacy Commissioners' Conference in October 2010. The *PbD* standard of designing protections in from the outset has also become a hallmark of privacy and security analyses of the Smart Grid and Smart Metering, as shown in Appendix A.

Privacy by Design is providing organizations with a means to, by considering privacy from the outset, achieve a positive-sum scenario – meeting both privacy and functionality requirements. The movement towards the Smart Grid and, in particular, smart metering, in its current nascent state, is at an ideal stage for the application of *Privacy by Design*. Below, we offer a number of recommendations for smart metering initiatives, based on the *Best Practices for Privacy on the Smart Grid*[11].

Recommendations

1) **Smart metering initiatives should feature privacy principles in the overall project governance framework and proactively embed privacy requirements into their design, in order to prevent privacy-invasive events from arising.**

[7] http://blogs.sfweekly.com/thesnitch/2010/12/smart_meters_west_marin.php
[8] http://www.oipc.bc.ca/news/2011Releases/NR_SmartMeters_28July2011.pdf
[9] http://www.consumentenbond.nl/morello-bestanden/209547/onderzoek_UvT_slimme_energi1.pdf.
[10] http://download.pwc.com/ie/pubs/smart_from_start.pdf
[11] http://www.privacybydesign.ca/content/uploads/2010/03/achieve-goldstnd.pdf

Utilities should conduct Privacy Impact Assessments (PIAs) or similar type assessments as part of the requirements and design stages of smart metering initiatives. Within this evaluation, two important considerations should be made. First, utilities should make a determination of what smart meter-based information is *required* to meet legitimate objectives (and at what level of identifiability), rather than of what information is made *available* by smart metering. Mechanisms should then be put in place to allow consumers to maintain control over any available, non-necessary information. Secondly, only the personal information necessary for the determined purposes should leave the consumer's home via the smart meter. In order to ensure that consumers always retains control over their data it is essential that they are fully informed about the data which leave their homes. They should have the possibility to determine which data is sent and to intervene if necessary.

Some research has shown that utilities may not need detailed energy consumption information about individual consumers to perform load balancing functions. To achieve as little personal data flow as possible utilities may use techniques such as anonymisation, pseudonymisation, or data aggregation[12]. Local gateways for individual buildings or small neighbourhoods, which allow the consumer to gain insight into their energy usage without the need for transmission of information about identifiable consumers to the utility, should be applied. Such gateways should generally not be externally-accessible and work with defined access protection profiles, while communication should be push-based (initiated by the gateway). Other measures, such as larger intervals between individual readings, can also prevent a detailed profile about the consumer's life-style from being generated. Of course, high technical standards for securely storing and accessing the data will be essential.

2) Smart meters should ideally protect privacy by default, with no action required on the part of the consumer

In order to ensure its presence, privacy should ideally be protected as the default condition. Privacy should be in a 'no action required' mode; consumer action should only be required for the *disclosure* of data exceeding core utility services, not the *protection* of personal information. At least two particular considerations should be made here. First, where multiple options (with regard to either the type of meter or its initial settings) are presented to the consumer, the default option should be the more privacy-protective one. Secondly, even where consumers have opted to have detailed consumption information collected by the smart meter, the informed, positive consent of those individuals should be sought prior to each separate use or disclosure of this information for non-primary purposes.

3) Privacy should be an essential design feature of smart meter systems and practices

As smart metering initiatives are seen in an increasing number of jurisdictions worldwide, a number of industry best practices and legislative requirements are under development. These will enhance the efforts of utilities and third-parties to create privacy-friendly practices for the collection, use and disclosure of smart meter-based information. Regulators should state the main principles that the consumer should have full transparency and the ability to control and determine the flow of personal data. Detailed patterns of an individual's energy consumption should only be accessible to the data subject, unless he or she shares them further.

However, privacy cannot be solely reliant on legislative or administrative protections; it should also be designed into the technology itself. As the point of collection, smart meters can play a clear role in defining what data will enter the larger Smart Grid ecosystem, and the form in which it will do so.

---

[12] For instance, see Kursawe, K., Danezis, G, and Johlweiss, M. (2011) Privacy-Friendly Aggregation for the Smart-Grid; and Jawurek, M., Johns, M., and Kerschbaum, F. (2011) Plug-in privacy for Smart Metering billing; both in Fischer-Hübner, S. and Hopper, N (Eds): *Proceedings of the 11th Privacy Enhancing Technologies Symposium*, Waterloo, ON, July 2011

4) Smart metering initiatives should avoid unnecessary trade-offs between privacy and other legitimate functionalities or organizational objectives

Privacy should not be considered to be 'at odds' with the functionality of smart meters. Consumers should not be forced into a choice between privacy and energy efficiency/conservation; utilities should ensure, through the use of *Privacy by Design*, that all legitimate objectives (including privacy) are met in smart metering initiatives.

5) Privacy and data security should be maintained end-to-end – full lifecycle protection

Smart meter-based information – particularly personally identifiable information – should be strongly protected, whether at rest or in transit. This requires the development and implementation of data protections at the smart meter itself (ensuring, to the extent possible, that the device is tamperproof, and that it does not store more data than necessary), during transmission of the data (encryption, anonymisation, identification and protection of metadata), and during processing and use (minimized access to data, ensuring third parties meet equivalent protection standards, secure destruction at end-of-life, etc.).

6) Smart metering initiatives should be visible and transparent, and should utilize accountable business practices; consumers should be assured that the technology operates in accordance with stated objectives

Utilities should be able to show that the methods used to incorporate privacy into their smart metering initiatives will meet the privacy requirements of the project. Ensuring such 'requirements traceability' between the foundational privacy principles and each stage of a smart metering initiative will ensure that the utility is ready for a third part audit at any time.

Informing consumers of the use to which personal information collected from smart meters will be put, and the establishment of a clear and accessible complaints process, are key objectives in achieving visibility and transparency. Consumers should be given the simple technical option to define access control profiles and thus determine who receives what personal information.

7) Smart metering initiatives should be designed to respect consumer privacy – keep it user-centric.

Consumers should be provided with, and educated about, all necessary information, options and controls to allow them to manage their energy consumption and their privacy.

8) Regulatory frameworks should foster the introduction and use of privacy-friendly smart meter and smart grid applications.

The concepts laid out in the recommendations above should be incorporated into national and international regulatory frameworks where this is not already the case.

APPENDIX A – Examples of *Privacy by Design* in Smart Grid consultation documents

- **Expert Group 2**: "If privacy is addressed at the design phase of the Smart Grid ('privacy by design'), it is possible to derive user and business friendly solutions"; "Be aware of future function creep and incorporate privacy and security considerations early on in the development by applying 'privacy (and security) by design' principles"[13]
- **Article 29 Working Group**: "Smart metering implementation should take place with privacy built in at the start, not just in terms of security measures, but also in terms of minimising the amount of personal data processed"[14]
- **European Commission**: "The Smart Grids Task Force has agreed that a 'privacy by design' approach is needed. This will be integrated in the standards being developed by the ESOs [European Standards Organizations]."[15]
- **Data Protection Commissioners of the Federation and of the Länder (Germany):** "Data protection must be guaranteed already when planning and designing the infrastructure for energy metering and the technical equipments."[16]
- **Public Interest Energy Research (PIER) Program:** "Privacy considerations must drive architectural and information flow design decisions within the network, as well as the policies that cover Smart Grid data held by the growing array of entities that will help reap the benefit of this investment. Because privacy must be embedded in technical design, it cannot be addressed adequately by policies created once technologies have matured."[17]
- **Trans-Atlantic Consumer Dialogue (TACD)**: "Encourage privacy and security by design, including data minimization, anonymisation, and aggregation, and models that focus on consumers' maintaining control of their utility consumption data."[18]
- **National Institute of Standards and Technology (NIST):** "With heavy reliance upon technology and information sharing, addressing privacy risks must be part of the business model today, and consideration of privacy impacts should be part of everyday business activities."[19]
- **Ontario (Canada) Minister of Energy Directive:** "Respect and protect the privacy of customers. Integrate privacy requirements into smart grid planning and design from an early stage, including the completion of privacy impact assessments."[20]
- **Center for Democracy and Technology & Electronic Frontier Foundation:** "Adopting privacy rules implementing the full set of [Fair Information Practices] now, at the beginning of Smart Grid deployment, will provide a sound and adaptable framework for designing privacy into the Smart Grid as it develops, giving utilities and innovators a solid framework upon which to build."[21]
- **Smart Grid Canada:** "The successful deployment of smart grid ultimately relies on consumer confidence and trust, privacy and other public concerns that threaten to undermine consumer confidence need to be addressed. It is an immediate priority to define the integrity issues, escalate the development of solutions and standards, and embed them into smart grid products and services deployed in Canada.[22]

---

[13] http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf
[14] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf
[15] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0202:FIN:EN:PDF
[16] Resolution of the 80th Conference of the Data Protection Commissioners of the Federation and of the Länder (Nov. 3-4, 2010), "Data protection in connection with digital metering and control of energy consumption." http://www.datenschutz-berlin.de/attachments/823/Appendix_2.pdf
[17] http://hes-standards.org/doc/SC25_WG1_N1475.pdf
[18] http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=294&Itemid=
[19] http://epic.org/privacy/smartgrid/NIST_Smartgrid_Priv_Guidelines.pdf
[20] http://www.wise.uwaterloo.ca/SmartGrid/Minister_directive_smart_grid_20101123.pdf
[21] http://www.eff.org/files/PoliciesandProcedures_15Oct2010_OpeningComment.pdf
[22] http://sgcanada.org/media/2011/04/Smart-Grid-Priorities-for-Canada-in-2011.pdf